Statement of FDCC Compliance

To perform a remote assessment for Federal Desktop Core Configuration (FDCC) compliance, the following changes must be made to the remote system to ensure a proper and complete analysis (steps apply to both Windows Vista and Windows XP systems unless otherwise noted):

- Enable Remote Registry – the Retina Vulnerability Scanner requires remote access to the target system's registry.
    - Click the Start button, select Run and enter the command "net start RemoteRegistry"
- Modify the following Security Options from the Local Security Policy settings to allow remote access
    - Click the Start button, select Run and enter the command "gpedit.msc".
    - From the GUI, go to "Computer Configuration" → "Security Settings" → "Local Policies" → "Security Options"
        - Set the option "Network access: Sharing and security model for local accounts" as: Classic – local users authenticate as themselves.
        - Set the option "Network security: LAN Manager authentication level" as: Send LM & NTLM – use NTLMv2 session security if negotiated.
- Disable the Windows Firewall settings to allow remote access
    - Click the Start button, select Run and enter the command "Regedit.exe".
        - Navigate to the following location: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall
        - Backup the key and then delete the "WindowsFirewall" branch.
    - From the GUI, go to "Computer Configuration" → "Administrative Templates" → "Network" → "Network Connections" → "Windows Firewall"
        - Modify all settings in both the "Domain Profile" and the "Standard Profile" to be "Disabled".
    - Click the Start button → go to the Control Panel → open "Windows Firewall" →select "Change settings" → select "Off (not recommended) and click OK.
- Disable UAC on Windows Vista target systems
    - Click the Start button → go to the Control Panel → open "User Accounts" → select "Turn User Account Control on or off" → unselect the "Use User Account Control (UAC) to help protect your computer" check box and click OK.

Retina Network Security Scanner is compliant with FDCC 1.2.

Statement of SCAP Implementation

Retina Network Security Scanner supports the following SCAP capabilities:

- Federal Desktop Core Configuration (FDCC) Scanner

- Authenticated Configuration Scanner
- Authenticated Vulnerability and Patch Scanner
- Unauthenticated Vulnerability Scanner

Retina's SCAP capabilities include the following standards: XCCDF, OVAL, CCE, CPE, CVE and CVSS.

When utilizing Retina Network Security Scanner's SCAP engine, users are able to import SCAP content (such as FDCC benchmarks) for interpretation and assessment of network devices. Retina provides an easy to use wizard that walks the user through the steps of selecting the desired content, providing information on the assets to be evaluated, and starting the assessment scan. The scan will then run without user intervention, and the user is alerted when it completes. The results from that assessment are then made available in both machine readable XML in OVAL and XCCDF formats as well as human readable reports. The machine and human readable output contains associated CVE, CPE, CVE and CVSS references as applicable.

Statement of CVE Implementation

Retina Network Security Scanner supports the use of Common Vulnerability and Exposures (CVE). CVE is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known problems.

Where applicable, vulnerability audits within Retina contain a related CVE identifier. This unique identifier can be used to correlate vulnerability information between other CVE compatible products or for referencing additional online information. CVE identifiers are displayed wherever vulnerability details are provided: while selecting audits for inclusion in an assessment, when viewing scan results within the user interface, and when exporting reports (both human readable and machine readable SCAP compliant reports). A link to the CVE website is also provided so that additional details can be viewed. The CVE identifier can be used to search for a particular vulnerability audit. Users can search directly by the CVE identifier, or they can browse through a list of CVE identifiers and CVE descriptions.

Retina Network Security Scanner is compliant with CVE.

Statement of CCE Implementation

Retina Network Security Scanner supports the use of Common Configuration Enumeration (CCE). CCE assigns unique entries to configuration guidance statements and configuration controls to improve workflow by facilitating fast and accurate correlation of configuration issues present in disparate domains.

Where applicable, configuration audits within Retina contain a related CCE identifier. This unique identifier can be used to correlate vulnerability information between other CCE compatible products or for referencing additional online information. CCE identifiers are displayed wherever vulnerability details are provided: while selecting audits for inclusion in an assessment, when viewing scan results within the user interface, and when exporting reports (both human readable and machine readable

SCAP compliant reports). The CCE identifier can be used to search for a particular configuration audit. The search results display all audits associated with the given CCE, allowing the user to then select the audit for inclusion within a vulnerability scan.

Retina Network Security Scanner is compliant with CCE version 5.0.

Statement of CPE Implementation

Retina Network Security Scanner supports the use of Common Platform Enumeration (CPE). CPE is a structured naming scheme for information technology systems, platforms, and packages.

When utilizing Retina's SCAP scan capabilities, content is consumed by the scanner and the definition files analyzed. If the supplied content includes a CPE identifier it will then be used in the XCCDF and OVAL compatible output as well as the human readable report. This unique identifier can be used to correlate platform details between other CPE compatible products or for referencing additional online information.

In addition to the SCAP CPE implementation, Retina uses numerous additional methods for determining the remote operating system of scan targets (registry, NetBIOS, SNMP, ICMP fingerprinting and TCP fingerprinting). Where possible, these methods will attempt to reference a corresponding CPE identifier to provide further information on the detected operating system.

Retina Network Security Scanner is compliant with CPE version 2.2.

Statement of CVSS Implementation

Retina Network Security Scanner supports the use of the Common Vulnerability Scoring System (CVSS). CVSS is a vendor agnostic, industry open standard designed to convey vulnerability severity and help determine urgency and priority of response.

Where applicable, vulnerability and configuration audits within Retina contain a related CVSS score. This score can be used to prioritize vulnerabilities discovered during an assessment and to help rank those vulnerabilities for appropriate remediation. CVSS details including overall score and the underlying metrics used to derive that score are displayed wherever vulnerability details are provided: while selecting audits for inclusion in an assessment, when viewing scan results within the user interface, and when exporting reports (both human readable and machine readable SCAP compliant reports). A link to the CVSS website is also provided so that score calculations can be analyzed and environmental vectors adjusted to produce a customized score.

Retina Network Security Scanner is compliant with CVSS version 2.0.

Statement of XCCDF Implementation

Retina Network Security Scanner supports the use of the eXtensible Configuration Checklist Description Format (XCCDF). XCCDF is a standard specification language for writing security checklists, benchmarks, and related documents.

When utilizing Retina's SCAP scan capabilities, content is consumed by the scanner and all XCCDF benchmark files are validated to ensure that they are both well formed and accurate for the selected assessment. The underlying scan engine then uses the XCCDF benchmarks to assist in the verification of the configuration and vulnerability information of the selected targets. Once the assessment has been completed, Retina will generate SCAP compliant output (both OVAL and XCCDF) based on the findings of the assessment. This output is provided in both machine readable format (XML) as well as human readable reports. The machine readable output can be used by other XCCDF compatible products for additional reporting.

Retina Network Security Scanner is compliant with XCCDF version 1.1.4.

Statement of OVAL Implementation

Retina Network Security Scanner supports the use of the Open Vulnerability and Assessment Language (OVAL). OVAL is an international, information security, community standard for defining vulnerability audits using XML.

When utilizing Retina's SCAP scan capabilities, content is consumed by the scanner and all related OVAL definitions are validated to ensure that they are both well formed and accurate for the selected assessment. The underlying scan engine then uses the OVAL definitions to verify the configuration and vulnerability information of the selected targets. OVAL definitions are processed natively by the scan engine and are not converted to an internal format for assessment. Retina then generates SCAP (both OVAL and XCCDF) output based on the findings of the assessment. . The machine readable output can be used by other SCAP compatible products for additional reporting.

Retina Network Security Scanner is compliant with OVAL version 5.5 and can process definitions related to the Microsoft Windows environment.